Security & Privacy
Implementing Appendix J of 800-53
Agenda

- Looking at Appendix J Control families
- How DOT is addressing them
- MARAD Progress report

- How this all is coming together in SP 800-53, Rev 4
Claire Barrett –

– DOT Chief Privacy Officer
– Member of the Privacy Controls Appendix Working Group

for her background information and current leadership in this effort.
Privacy Controls Catalog

- The Administrative, technical & physical safeguards
- Can be implemented at multiple levels across the organization form the department down to individual programs & offices
- Selection and implementation includes contributions from the Senior Agency Officer for Privacy, Department CIO, Agency CIOs, Privacy and Security Officers and legal counsel.

In General

- Privacy Controls are implemented “From Above” and inherited by individual programs and systems
Some Definitions

- **Privacy:**
  - The appropriate use of personal information under the circumstances. What is appropriate depends on context, law and individual expectations also the right on an individual to control the collection, user & disclosure of personal information.

- **Data Protection**
  - The management of personal information.

- In the US, we refer to privacy laws; in the EU & other countries, these are often referred to data protection laws.
Definitions

- **Controllers** –
  - the organization(s) which determine the purposes and means of processing personal information

- **Processors**
  - Perform this processing on behalf of the controller

These are sometimes referred to as **data owners** and **data stewards**.
Why Get The IT Organizations Involved?

Privacy is the “WHAT”

Security is the “HOW”
Privacy Controls Families

- Transparency
- Individual Participation & redress
- Authority & Purpose
- Data Minimization & retention
- Use Limitation
- Data Quality & Integrity
- Security
- Accountability, Audit, and Risk Management
Where DID DOT Start

- Privacy Guidance SharePoint Site
- Training
- System of Record reviews
- Privacy Newsletter Weekly
- Change in incident reporting workflow
- Department-wide review of all Privacy Documentation
  - Review of all Systems of Records Notices
  - Consolidation of applicable notices to the department level
  - Rewrite of System of Records Notices
  - Republication in Federal Register

- Department review of all Agency and OCIO Privacy Threshold Assessments prior to publication
- Department review and approval/republication of Privacy Impact Assessments

This presentation is the property of the U.S. Government and may not be reproduced or distributed without credit to the U.S. Department of Transportation.
Training

- **On Site IAPP training**
  - Offered to all Agencies IT, administration and legal staff
  - Included both international and domestic regulations and practices, along with the security protections applicable.
  - Included testing for both the CIPP & CIPP/G certifications.
  - Did not require you to obtain the certification to be an agency Privacy officer, but wanted this common body of knowledge to be disseminated widely throughout the Department
Privacy Web Site – Internal & External

- Rework to provide access to all Department SORN, PIA and other privacy documentation
- Includes additional information on Department privacy direction and mission
- Includes Department information on access and redress for individuals.
- Internally, includes a weekly newsletter on incidents & events in the public & private sector, training opportunities and awareness items.
Forms Management

- Data Collection forms being made available on line with links to appropriate Systems of record & privacy notices

- Forms to include acceptance of data collection & sharing.
Individual Participation & Redress

- Assuring that the individuals right to consent, access, and redress is clearly articulated in All DOT Systems of record Notices

- Creation of Single Request Service: One location at the OCIO level where all Privacy requests move through
  - Single published address
  - Email
  - Phone
  - Web presence
Authority to Collect & Purpose

- Spelled out in the SORs

- As part of our transparency effort we are making our usage statements clear and individual friendly
  - Less “regulaese”
  - Simple statements of intent.
Data Minimization & Retention

- Review & rework of our records retention policy & practices.
  - Review completed in March, 2012

- Clarification and specification of our retention policy in the SONs and Privacy documentation (and the SSPs)

- Department-wide decisions on data destruction.
Use Limitations

- New Contract language for service and purchases
- Revision of Memorandum & Sharing agreements
- Mapping of data stores and possible co-mingling.
- Auditing of use
- Training of Design & Development staff
Data Quality & Integrity

- “Data Provenance”

- Requirements for integrity & quality being added to SDLC requirements & stages

- Identification of primary source for critical data stores

- Ranking of Data quality
Integration of privacy issue in full enterprise view
- Inventory of Privacy Information Assets
- Consolidation & reduction of Privacy repositories

Integration of privacy considerations into Incident Response process and tools
 Department Privacy Governance program

 New process and documentation of Risk Assessments to include privacy considerations

 New online training in development for all employees, contractors & others
  – Specialized training for privacy handling.
MARADs Special Challenges

- Public Information
- Mariner Information
- USMMA
MARAD’s Progress

- 35 Systems of Record Notices under Review – July 1, 2012
- Update and Re-submission by Dec 2012
- Privacy training provided to all system Owners, Program executives
  - Privacy training in planning for all, including Midshipman for FY2013.
- Review and modification of data sharing Agreements.
- Identification and protection of single user repositories of privacy information
SP800-53, Rev 4 states that these control families are not mandatory but are Best Practices.

The inclusion of “Privacy” in the name of the revised document is an indicator of the importance of inclusion in our Risk Management Framework.

There is no solid line between manual & electronic privacy policy and practice.

New technology will continue to challenge us in the privacy arena.
Questions?
Shelly Nuessle
Information System Security Manager
Maritime Administration
1200 New Jersey Ave, SE
Washington DC, 20590

shelly.nuessle@dot.gov
202-366-1104